Patent claims

1. Method of authentication, wherein a client (CL) requests a file from a server (SV), whereby the client and the server share a common secret value (S) and thereby belong to an accepted group, and whereby

the client forms a first message (M1) comprising

- a filename (FN),

- a nonce (N) which is associated with the given filename (FN),

- a first hash value (H(S^FN); 10) according to a first hash function (H1, H2) formed from the filename (FN) and the secret value (S).

2. Method according to claim 1, wherein the server

- extracts the filename (FN) of a received first message (M1),

- extracts the first hash value (10),

- forms a value of the received filename (FN) and the secret value (S),

- forms a second hash value (H(S^FN); 20) according to the first hash function (H1, H2) formed from the value of the filename (FN) and the secret value (S),

- compares the first hash value (10) with the second hash value (20) and if the values are the same, establishes that the first message (M1) stems from a client belonging to the accepted group, otherwise establishes that the client does not belong to the accepted group.

3. Method according to claim 1 or 2, wherein the server responds to the request from the client by forming a second message (M2) comprising

- a file (F) corresponding to the requested filename (FN),

- the received nonce (N) which is associated with the given filename (FN),

- a third hash value (H(S^FN); 30) according to a second hash function (H3, H4) formed from the value of the received nonce (N) and the secret value (S).

4. Method according to claim 3, wherein the client

- extracts the file (F) of the received second message (M2),

- extracts the third hash value (30) from the second message,

- forms a value of the nonce (N) associated with the filename (FN) and the secret value (S),

- forms a fourth hash value (H(S^N); 40) according to the second hash function (H3, H4) formed from the value of the nonce (N) associated with the requested filename and the secret value (S),

- compares the third hash value (30) with the fourth hash value (40) and if the values are the same establishes that the second message (M2) stems from a server belonging to the accepted group, otherwise establishes that the server does not belong to the accepted group.

5. Method according to claim 3 or 4, wherein the first hash function (H1, H2) is the same as the second hash function (H3, H4).

6. Method according to any previous claim wherein, the inputs to any respective hash function (H1, H2) are concatenated.

7. Client sharing a common secret value (S) with a server, the client and the server thereby belonging to an accepted group, whereby

the client forms a first message (M1) comprising

- a filename (FN),

- a nonce (N) which is associated with the given filename (FN),

- a first hash value (H(S^FN); 10) according to a first hash function (H1, H2) formed from the values of the filename (FN) and the secret value (S), and whereby

the client receives a second message from the server, the client

- extracting a file (F) of the received second message (M2),

- extracting a third hash value (30) from the second message,

- forming a value of the nonce (N) and the secret value (S),

- forming a fourth hash value (H(S^N); 40) according to a second hash function (H3, H4) formed from the value of the nonce (FN) associated with the requested filename and the secret value (S),

- comparing the third hash value (30) with the fourth hash value (40) and if the values are the same establishing that the second message (M2) stems from a server belonging to the accepted group, and if otherwise, establishing that the server does not belong to the accepted group.

8. Server sharing a common secret value (S) with a client, the client and the server thereby belonging to an accepted group, whereby the server receives a first message from the client, the server

- extracting the filename (FN) from the received first message (M1),

- extracting a first hash value (10) from the received first message (M1),

- forming a value of the received filename (FN) and the secret value (S),

- forming a second hash value (H(S^FN); 20) according to the first hash function (H1, H2) formed from the value of the filename (FN) and the secret value (S),

- comparing the first hash value (10) with the second hash value (20) and if the values are the same establishing that the first message (M1) stems from a client belonging to the accepted group, otherwise establishing that the client does not belong to the accepted group.

9. Server according to claim 8, wherein the server responds by sending a second message (M2) comprising

- a file (F) corresponding to the requested filename (FN),

- a third hash value (H(S^FN); 10) according to a second hash function (H3, H4) formed from the value of the received nonce (N) associated with the filename (FN) and the secret value (S).